CHAPTER 10

SECURITY

"You have been given two ears, two eyes, and but one tongue–to the end that you should hear and see more than you speak."

This chapter contains information about the security of documents and personnel in the Navy. The information will help you to become familiar with the individuals within the chain of command who are responsible for making sure security requirements are fulfilled. The chapter also covers security briefings and debriefings.

THE NAVY SECURITY PROGRAM

The basis of the information and personnel security program is the fact that there is official information truly essential to the national security that requires control of its dissemination so the information will not be used to the detriment of the United States. To protect this information from disclosure to any persons except those whose official duties require knowledge and possession and who have been determined to be trustworthy, it is classified. A level of classification is assigned from which flows standards for protection under the varying conditions that may arise in connection with its use, dissemination, storage, transmission, and disposal. Only that information that is truly essential to the national security maybe classified, and then only to the extent and for the period of time necessary.

All personnel who have been granted access to classified material must be knowledgeable as to security orientation, education, and training. When the Navy security program is in place and working as it should be, it will accomplish the following goals:

- Familiarize all personnel who are granted access to classified information with proper security measures necessary in performing their duties
- Remind all levels of command of their responsibility for ensuring that classified information is effectively and economically safeguarded
- Ensure conscientious and willing compliance with security regulations, procedures, and practices
- Remind commands of their responsibilities in proper classification, upgrading, downgrading, and declassification procedures as outlined in the *Department of the Navy Information and Personnel Security Program Regulation,* OPNAVINST 5510.1H
- Inform personnel who have access to classified material of the hazards involved due to unauthorized disclosure and impress on these personnel their responsibility in protecting classified documents
- Inform personnel of their responsibility to report attempts by foreign agents to obtain U.S. classified information
- Familiarize personnel with the techniques and devices used by foreign agencies to obtain classified U.S. information
- Advise personnel against using the telephone as a means of transmitting or discussing classified material
- Make personnel aware of the disciplinary action that may result from unauthorized disclosure of classified documents

RESPONSIBILITY

The Secretary of the Navy (SECNAV) is responsible for establishing and maintaining an information security program and a personnel security program in compliance with the provisions of Executive orders, public laws, National Security Council, Department of Defense, and other security directives regarding the protection of classified information, acceptance and retention of personnel, and assignment to sensitive duties.

The Chief of Naval Operations (CNO) is responsible to SECNAV for information and personnel security. The Special Assistant for Naval Investigative Matters and Security (OP-09N) has been designated as the official primarily responsible for making sure that there is an effective program and that it complies with all the directives issued by higher authority.

Commanding officers are held responsible for the proper indoctrination of personnel in safeguarding classified material. However, you, as the senior YN in

your office, are responsible for proper indoctrination of personnel under your supervision. You must be sure your personnel are fully aware of regulations and execute a policy of strict compliance with all security regulations at all times.

Effective security is accomplished when you recognize, understand, and apply the security requirements that prevent compromise and subversion. Some individuals who work with classified information on a daily basis may become careless about using proper safeguard measures. When you see this happen in your office, take corrective action immediately.

EFFECTIVE SECURITY

The primary objective in organizing and conducting an effective security program that should be impressed on your personnel is that security is not something separate and apart from their other duties. It is a natural element of every duty they perform.

An effective security program will help you to make your personnel security conscious at all times. You can use various approaches to organizing a security program that have real meaning and create a lasting impression on your personnel. Posters, cartoons, charts, and films are effective tools if properly used.

When you use posters, place them in areas of maximum travel and always at eye level. Use various types and rotate them often to combat boredom. People become security conscious only when you stimulate their interest and provide motivation for personal involvement.

When you have instilled a sense of self-responsibility in your personnel, a trait that eliminates carelessness, ignorance, or plain indifference, you have accomplished security consciousness.

Effective security can only be achieved when personnel know how, when, and with whom to discuss classified information.

BRIEFINGS

Security education/briefings fall into the following categories:

- Indoctrination
- Orientation
- On-the-job training
- Annual refresher briefings
- Counterespionage briefings
- Special briefings
- Debriefings

INDOCTRINATION

Everyone who enters the Navy and the Marine Corps needs to have a basic understanding of what classified information is and why and how it is protected. This basic indoctrination is done during training at the time of accessiom nose who don't go through a formal training period are indoctrinated by the receiving command.

It is not enough to make sure an initial indoctrination briefing is accomplished for new personnel; you must also make sure periodic briefings are conducted for all personnel having access to classified information In addition, security briefings may be appropriate when:

- an abnormal number of security violations occur.
- there is an increase in quantity or sensitivity of classified information being handled.
- the mission of a command increases in terms of security risk involvement (personnel or physical).

ORIENTATION

Orientation briefings are a must for personnel whose job requires access to classified material. The briefing should be conducted as soon as possible after an individual reports aboard and before he or she is granted access to classified information. Orientation briefings are also necessary for personnel who, although not required to have access to classified material, are closely associated with cleared personnel or who are attached to a command that has a primary mission that involves highly classified material and information. The orientation briefing places emphasis on the following factors:

- Personnel having knowledge of classified defense information must not disseminate it until it has been determined that the recipient has the appropriate security clearance and needs the information to perform his or her official duties. Each person has the responsibility for making this determination.

- Individuals may not have possession of classified information unless they have the necessary clearance and a need for the information in the performance of their duties.

- Individuals must be made keenly aware of their moral and legal responsibility y for any classified material or Information they may have in their possession. Individuals are required to make sure such material or information is given the degree of protection that it requires.

- Individuals must be made aware of the possibility of espionage and subversion attempts and the defensive steps that they must take against such attempts.

- Personnel must not discuss classified information on the telephone.

ON-THE-JOB TRAINING

Supervisors must make sure subordinates know the security requirements. Supervision of the on-the-job training process is critical. Leaving subordinates to learn by trial and error is costly to security, and so is assuming they know how classified information is to be protected. Compromise reports often reveal that fault lies with the supervisor who negligently or incorrectly assumed that subordinates knew what they were supposed to do. Examples include sending people on burn (destruction) detail without instructing them on proper destruction methods; assigning people to mail rooms without training them in preparation and transmission of classified material; or designating Top Secret control officers without reviewing control requirements.

REFRESHER BRIEFINGS

Once a year, all personnel who have access to classified information must receive a refresher briefing or equivalent training by supervisory personnel designed to enhance security awareness. The annual refresher briefing or equivalent training may be addressed to the entire command on general security matters, changes in policies, or procedures. It is unlikely that it will be possible to schedule everyone in the command at the same time. The refresher briefing will probably be more effective if it is tailored for a particular group. For example, brief those who are most likely to travel on command business. For clerical personnel, concentrate on the preparation of classified material. People who draft classified documents should be briefed on procedures for classifying and marking material.

COUNTERESPIONAGE BRIEFINGS

Once every 2 years, personnel who have access to material classified Secret or above must be given a counterespionage briefing by a Naval Investigative Service (NIS) agent. The security manager is responsible for arranging for the briefing with the local NIS office. A list of NIS components are listed in OPNAVINST 5510.1H appendixes.

SPECIAL BRIEFINGS

A special briefing covers a specific topic or problem and is given to a designated group. This type of briefing is often longer and more detailed than most other briefings. Special briefings are used to acquaint personnel with particular enemy capability. Some examples of such briefings are as follows:

- Foreign travel briefing
- NATO briefings
- Single-integrated operational plan extremely sensitive information (SIOP-ESI)
- Sensitive compartmented information (SCI)

Foreign Travel Briefings

Sometimes individuals are required to travel through certain foreign countries or when representatives of certain foreign countries are expected to participate in a meeting, the commanding officer must make sure the individual who is going to travel undergoes a defensive foreign travel briefing. Individuals who frequently travel (more than once a month) or attend meetings or host meetings for foreign visitors need not be briefed at each occasion. However, such individuals must be provided a thorough briefing at least once every 6 months and a general reminder of security responsibilities before each such activity. Individuals intending cruises on Soviet ships, which have recently become available, also require this precautionary briefing. In the interest of national security, and when deemed appropriate by the commanding officer, dependents may also be provided with the same briefing. It should place special emphasis on the various areas of interest to hostile intelligence services, the techniques used by these services, and on the nature of conduct or activity that could place a person in a compromising situation.

When the individual returns, he or she must be debriefed to provide the opportunity to report any

incident–no matter how insignificant it might have seemed-that could have security implications. A record should be maintained on individuals given the foreign travel briefing for follow-up.

Special Access Programs

Any program requiring additional security protection and handling measures; special investigative, adjudicative and clearance procedures; reporting procedures; or formal access lists is considered a special access program. These programs require special briefings before access may be granted.

- NATO-Individuals who are to have access to NATO information must be briefed on NATO security procedures by the NATO security officer. See OPNAVINST C5510.101.

- Single-integrated operational plan extremely sensitive information (SIOP-ESI)—A special briefing is given by an individual with SIOP-ESI access and is based on OPNAVINST S5511.35. A briefing and debriefing certificate is issued in the form recommended in DOD 5200.2-R.

- Sensitive compartmented information (SCI)–The special security officer (SSO) is responsible for briefing those individuals who are to have access to SCI.

Additional special access programs are listed in OPNAVINST 5510.1H. Special access programs cannot be established within the Department of the Navy without prior approval.

DEBRIEFINGS

When personnel no longer require access to classified material, are transferred, separated from active duty, or inadvertently gain substantive access to information that they were not eligible to receive, the commanding officer must make sure a security debriefing is conducted. The purpose of this debriefing is to inform the individuals of their responsibility in protecting classified material they have knowledge of, and it serves as a reminder that the persons are to report to proper authorities any attempt by unauthorized individuals to obtain classified information that they may possess.

DEBRIEFING STATEMENT

The Security Termination Statement, OPNAV Form 5511/14 (fig. 10-1), must be executed by civilian and military personnel including senior officials (flag and general officers and senior executive service and equivalent positions) when any of the following events occurs:

- An individual terminates active military service or civilian employment or is temporarily separated for a period of 60 days or more including sabbaticals and leave without pay.
- A limited access authorization expires.
- A security clearance is revoked for cause.
- A security clearance is administratively withdrawn.

When a security termination statement has been executed, the witness to the signature must sign the security termination statement. If someone refuses to execute the security termination statement, the individual will be debriefed anyway, before a witness if possible, stressing the fact that refusal to sign the security termination statement does not change the individual's obligation to protect classified information from unauthorized disclosure. The statement will be annotated to show the identity and signature of the witness, if one was present, and that the individual was debriefed, but refused to sign. A copy will be forwarded to CNO (OP-09N). Failure to execute the statement is reported immediately to the Deputy Under Secretary of Defense for Policy via CNO (OP-09N).

When the action described above has been accomplished, the security termination statement becomes part of the individual's record. The original security termination statement will be placed in the individual's official personnel record for permanent retention except for the following:

- When the security clearance of a marine has been revoked for cause, the original is forwarded to the Commandant of the Marine Corps (MSRB) as an enclosure to the revocation letter, and a copy is placed in the service record.

- When the security termination statement has been executed at the conclusion of a limited access authorization, the original is retained in command tiles for 2 years.

A security termination statement is not executed when a member is being transferred from one command to another. A debriefing is given and the member is told that all classified material must be returned. Any

SECURITY TERMINATION STATEMENT
OPNAV 5511/14 (REV. 7-78)
S/N 0107-LF-056-1171

Enter name and address of appropriate Naval or Marine Corps activity obtaining statement.

Commanding Officer
Fleet Intelligence Center Pacific
Honolulu, HI 96860-5000

1. I HEREBY CERTIFY that I have conformed to the directives contained in the Information Security Program Regulation (OPNAV Instruction 5510.1), and the Communications Security Material System Manual (CMS-4) in that I have returned to the Department of the Navy all classified material which I have in my possession.

2. I FURTHER CERTIFY that I no longer have any material containing classified information in my possession.

3. I shall not hereafter communicate or transmit classified information orally or in writing to any unauthorized person or agency. I understand that the burden is upon me to ascertain whether or not information is classified and agree to obtain the decision of the Chief of Naval Operations or his authorized representative on such matters prior to disclosing information which is or may be classified.

4. I will report to the Federal Bureau of Investigation or to competent naval authorities without delay any incident wherein an attempt is made by an unauthorized person to solicit classified information.

5. I Paul Tee Boat have been informed and am aware that Title 18 U.S.C., Sections 793-799, as amended and the Internal Security Act of 1950 prescribe severe penalties for unlawfully divulging information affecting the National Defense. I certify that I have read and understand appendix F of the Information Security Program Regulation OPNAV Instruction 5510.1. I have been informed and am aware that certain categories of Reserve and Retired personnel on inactive duty can be recalled to duty, under the pertinent provisions of law relating to each class for trial by court-martial for unlawful disclosure of information. I have been informed and am aware that the making of a willfully false statement herein renders me subject to trial therefor, as provided by Title 18 U.S.C. 1001.

6. I have/have not received an oral debriefing.

SIGNATURE OF WITNESS	SIGNATURE OF EMPLOYEE OR MEMBER OF NAVAL OR MARINE CORPS SERVICE *(Fill in first, middle, and last name If military, indicate rank or rate. If civilian indicate grade.)*
Water T. Door	Paul Tee Boat LIZ
TYPE OR PRINT NAME OF WITNESS Water T. Door	DATE 15 Apr 93

Figure 10-1.-Security Termination Statement, 0PNAV Form 5511/14.

material personally complied, such as classified notes or notebooks, for which the member has a legitimate need at the new command will be forwarded through official channels.